SPG U-M Standard Practice Guide

Information Security Incident Reporting

601.25

Applies to: All Faculty and Staff

Search this page

I. Overview

It is the policy of the University of Michigan to handle information security incidents so as to minimize their impact on the confidentiality, integrity, and availability of the university's systems, applications, and data. An effective approach to managing such incidents also limits the negative consequences to both the university and individuals, and improves the university's ability to promptly restore operations affected by such incidents.

It is especially important that serious information security incidents that may result in disruptions to important business processes are promptly communicated to the appropriate university officials so that they are involved early in decision-making and communications. In addition, compliance with various federal and state regulations requires expeditious reporting of certain types of incidents.

While information security incidents are not always preventable, appropriate procedures for incident detection, reporting and handling, combined with education and awareness of the U-M community, can minimize their frequency, severity, and potentially negative individual, operational, legal, reputational, and financial consequences.

The goals of establishing a successful incident management capability include:

A. Mitigating the impact of IT security incidents.

B. Identifying the sources and underlying causes of IT security incidents and unauthorized disclosures to aid in reducing their future likelihood of occurrence.

C. Protecting, preserving, and making usable all information regarding the incident or disclosure as necessary for forensic analysis and notification.

D. Ensuring that all parties are aware of their responsibilities regarding IT system security incident handling.

E. Protecting the reputation of the university.

II. Definitions

A. An information security incident is a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of information; interference with information technology operations; or significant violation of responsible use policy, (as defined in Responsible Use of Information Resources (SPG 601.07). Examples of information security incidents

- Computer system intrusion
- Unauthorized or inappropriate disclosure of sensitive institutional data
- Suspected or actual breaches, compromises, or other unauthorized access to U-M systems, data, applications, or accounts

- Unauthorized changes to computers or software
- Loss or theft of computer equipment or other data storage devices and media (e.g., laptop, USB drive, personally owned device used for university work) used to store private or potentially sensitive information
- Denial of service attack or an attack that prevents or impairs the authorized use of networks, systems, or applications
- Interference with the intended use or inappropriate or improper usage of information technology resources.

While the above definition includes numerous types of incidents, the requirement for central security incident reporting, regardless of malicious or accidental origin, is limited to serious incidents as defined below.

Occurrences such as incidental access by employees or other trusted persons where no harm is likely to result will usually not be considered information security incidents.

B. A serious incident is an incident that may pose a substantial threat to university resources, stakeholders, and/or services. An incident is designated as serious if it meets one or more of the following criteria:

- Involves potential, accidental, or other unauthorized access or disclosure of sensitive institutional information (as defined below)
- Involves legal issues including criminal activity, or may result in litigation or regulatory investigation
- May cause severe disruption to mission critical services
- Involves active threats
- Is widespread
- Is likely to be of public interest
- Is likely to cause reputational harm to the university

C. Sensitive information is defined in Institutional Data Resource Management Policy, (SPG 601.12) as information whose unauthorized disclosure may have serious adverse effect on the university's reputation, resources, services, or individuals.Information protected under federal or state regulations or due to proprietary, ethical, or privacy considerations will typically be classified as sensitive. Sensitive information includes personally identifiable information such as protected health information (PHI), Social Security numbers, credit card numbers, and any other information designated as sensitive by university data stewards.

III. Scope

This policy is platform and technology neutral, and applies to the entire university, including the Ann Arbor campus, Health System, U-M Dearborn, U-M Flint, Athletics, and all affiliates. Specifically, the scope of this policy encompasses:

- Faculty, staff, and all units;
- Third-party vendors who collect, process, share or maintain university institutional data, whether managed or hosted internally or externally;
- Personally owned devices of members of the U-M community that access or maintain sensitive institutional data.

IV. Policy

A. All users of university IT resources must report all information security incidents to their IT security provider or security unit liaison.

B. Any event that appears to satisfy the definition of a serious information security incident must be reported to IIA.

C. It is expected that incident reporting, from identification to reporting to IIA (if necessary), will occur within 24 hours.

D. Some information security incidents may also be criminal in nature (e.g., threats to personal safety or physical property) and should immediately be reported to the U-M Division of Public Safety and Security concurrent with the incident notification described in section VII of this policy.

E. To avoid inadvertent violations of state or federal law, individuals and departments may not release information, electronic devices, or electronic media to any outside entity, including law enforcement organizations, before making the notifications required by this policy.

F. Privacy and Confidentiality of Sensitive Information:

- Information related to campus security information security incidents is classified as sensitive under SPG 601.12.
- When university staff report, track, and respond to information security incidents, they must protect and keep confidential any sensitive information.
- Incident data retained for investigation will exclude any sensitive information that is not required for incident response, analysis, or by law, regulation, or university policy.

V. Roles and Responsibilities

A. *The University Chief Information Security Officer* is the ultimate authority for interpretation and implementation of this policy, as well as for coordinating serious information security incident communications. The Office of the University Chief Information Security Officer will retain relevant records and evidence pertaining to all serious incidents for a period of three years after the occurrence of the event. For incidents involving unauthorized disclosure of PHI, records will be retained for six years.

B. *Information and Infrastructure Assurance* (IIA) will oversee, coordinate, and guide the incident management process to promote a consistent, efficient, and effective response, including compliance with applicable breach notification laws and regulations. IIA staff serve as the information security provider for Information and Technology Services and all MiWorkspace units.

In addition, IIA shall:

1. Convene, when appropriate, a multi-department Computer Security Incident Response Team (CSIRT).
2. Collaborate and coordinate with other university offices including applicable compliance offices.
3. Take appropriate steps to preserve forensic evidence.
4. Lessons learned meetings will be conducted for all serious information security incidents to review the effectiveness of the incident handling process, prevent recurrence of similar incidents, and identify potential improvements to existing security controls and practices.
5. Conduct ongoing information security incident reporting education and awareness for the U-M community.

C. *Users of University Information Technology Resources:* All faculty, staff, and workforce members must report serious information security incidents to the ITS Service Center for MiWorkspace units and the ITS Service Center and their unit's security unit liaison for non-MiWorkspace units within 24 hours of becoming aware of the incident.

D. *Security Unit Liaisons:* The Security Unit Liaison is a staff member that has been designated by the unit dean or director to provide unit oversight of information security, communicate and coordinate related activities with Information and Infrastructure Assurance (IIA), evaluate and respond to non-serious incidents, and coordinate unit response to risk assessments and audit requests. Liaisons also develop and implement unit-level policies, procedures, communications, and educational awareness programs consistent with university-wide guidance.

1. Security unit liaisons or their designees must report suspected serious incidents (reported to or identified by them) within the 24 hour timeframe. When an incident involves the types of sensitive information below, the liaisons must also report the incident to the following parties:

    - **If an incident involves protected health information (PHI)**, security unit liaisons must report the incident to Information and Infrastructure Assurance (IIA) at security@umich.edu *and* the University HIPAA Privacy Director at UMHS-Compliance-IT-Sec@med.umich.edu.
    - **If an incident involves any human subject research information**, security unit liaisons must report the incident to IIA at security@umich.edu *and* the Office of Research (UMOR) UMOR-IT-Sec@umich.edu. UMOR will report the incidents to the appropriate Institutional Review Board and the IRBs will alert research teams, as needed.

- **If an incident involves *both* protected health and human subject research information**, UMOR (UMOR-IT-Sec@umich.edu), the University HIPAA Privacy Director (UMHS-Compliance-IT-Sec@med.umich.edu), and IIA (security@umich.edu) should receive the report at the same time and work together on any required follow-up. UMOR will report the incidents to the appropriate IRB, and the IRBs will alert research teams, as needed.
- **If an incident involves payment card information (PCI),** a U-M merchant must report the incident to the Treasurer's Office at merchantservices@umich.edu and IIA at security@umich.edu.

2. Security unit liaisons and associated unit IT staff will appropriately support IIA staff in incident handling and post-incident investigations and will evaluate and respond to information security incidents in accordance with university and unit policies and procedures.

3. Security unit liaisons for non-MiWorkspace units will, as necessary, develop and implement unit-level policies, procedures, communications, and educational programs that are consistent with this university-wide incident reporting policy.

E. The University HIPAA Privacy Officer, UMOR, and the Treasurer's Office will inform IIA of serious incidents reported to them.

F. *Third Party Vendors and Contractors:* U-M has an ownership, stewardship or custodial interest in all university data, regardless of how or where it is stored, transmitted, or processed. The reporting requirements of this policy apply to third parties that are contractually bound to limit the access, use, or disclosure of U-M information assets. These third party vendors or entities shall report potential or actual incidents to the university per the terms of their contract and/or the university's data protection addendum.

VI. Violations and Sanctions

Violations of this policy may result in disciplinary action up to and including suspension or revocation of computer accounts and access to networks, non-reappointment, discharge, dismissal, and/or legal action. Discipline (SPG 201.12)provides for staff member disciplinary procedures and sanctions. Violations of this policy by faculty may result in appropriate sanction or disciplinary action consistent with applicable university procedures. If dismissal or demotion of qualified faculty is proposed, the matter will be addressed in accordance with the procedures set forth in Regents Bylaw 5.09. In addition to U-M disciplinary actions, individuals may be personally subject to criminal or civil prosecution and sanctions if they engage in unlawful behavior related to applicable federal and state laws.

VII. Reporting Incidents

- Information and Infrastructure Assurance (IIA) - security@umich.edu
- Incidents involving PHI: University HIPAA Officer - UMHS-Compliance-IT-Sec@med.umich.edu
- Incidents involving human subject research: Office of Research - UMOR-IT-Sec@umich.edu and Institutional Review Boards – irbhsbs@umich.edu or irbmed@umich.edu
- Incidents involving payment card information (PCI): Treasurer's Office –merchantservices@umich.edu
- Incidents that may also be crimes or threats to personal safety: Division of Public Safety and Security – (734) 763-8391

VIII. Related Policies

- Responsible Use of Information Resources (SPG 601.07)
- Institutional Data Resource Management (SPG 601.12)
- Information Security Policy (SPG 601.27)
- Report an IT Security Incident, Safe Computing

Attachment	Size

Printable PDF of SPG 601.25, Information Security Incident Reporting Policy 2.89 MB

SPG number:
601.25

Date issued:
July 10, 2006

Last updated:
June 29, 2016

Next review date:
June 29, 2021

Applies to:
All Faculty and Staff

Owner:
Office of the Executive Vice President and Chief Financial Officer, the Office of the Provost and Executive Vice President for Academic Affairs, and the Office of the Executive Vice President for Medical Affairs

Primary contact:
Office of the CIO

Related policies:
Information Security Policy
Institutional Data Resource Management Policy
Responsible Use of Information Resources

Related links:
Report an IT Security Incident, Safe Computing
Information Technology Policies and Standards